

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-007533  
 (43)Date of publication of application : 08.01.2004

(51)Int.CI. H04N 5/92  
 G06F 12/14  
 G09C 1/00

(21)Application number : 2003-092358 (71)Applicant : TOSHIBA CORP  
 (22)Date of filing : 28.03.2003 (72)Inventor : SATO JUN  
 TERAUCHI TORU

(30)Priority

Priority number : 2002097757 Priority date : 29.03.2002 Priority country : JP

**(54) DATA STRUCTURE OF MULTIMEDIA/FILE/FORMAT, METHOD AND DEVICE FOR DATA ENCRYPTION, AND METHOD AND DEVICE FOR DECRYPTING ENCRYPTED DATA**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide the data structure of multimedia/files/formats, which is allowed to efficiently access a prescribed position of contents data, an encrypting method for encrypting the data and a decrypting method for decrypting the encrypted data.

**SOLUTION:** In the data structure of multimedia/files/formats, a movie box and a media data box are prepared. Respective boxes are provided with non-encrypted sizes/fields, types/fields and boxes/data/fields. Information data concerned with non-encrypted or encrypted multimedia data are stored in the box/data/field of the movie box and encrypted multimedia/data are stored in the box data/field of the media data box.



**LEGAL STATUS**

[Date of request for examination] 28.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

**This Page Blank (uspto)**

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

**This Page Blank (uspto)**

(19)日本国特許庁(JP)

## (12)公開特許公報(A)

(11)特許出願公開番号

特開2004-7533

(P2004-7533A)

(43)公開日 平成16年1月8日(2004.1.8)

(51)Int.Cl.<sup>7</sup>

H04N 5/92

G06F 12/14

G09C 1/00

F 1

H04N 5/92

G06F 12/14

G09C 1/00

H

テーマコード(参考)

5B017

5C053

5J104

審査請求 有 請求項の数 18 O L (全 22 頁)

(21)出願番号 特願2003-92358 (P2003-92358)  
 (22)出願日 平成15年3月28日 (2003. 3. 28)  
 (31)優先権主張番号 特願2002-97757 (P2002-97757)  
 (32)優先日 平成14年3月29日 (2002. 3. 29)  
 (33)優先権主張国 日本国 (JP)

(71)出願人 000003078  
 株式会社東芝  
 東京都港区芝浦一丁目1番1号  
 (74)代理人 100058479  
 弁理士 鈴江 武彦  
 (74)代理人 100091351  
 弁理士 河野 哲  
 (74)代理人 100088683  
 弁理士 中村 誠  
 (74)代理人 100108855  
 弁理士 蔡田 昌俊  
 (74)代理人 100084618  
 弁理士 村松 貞男  
 (74)代理人 100092196  
 弁理士 橋本 良郎

最終頁に続く

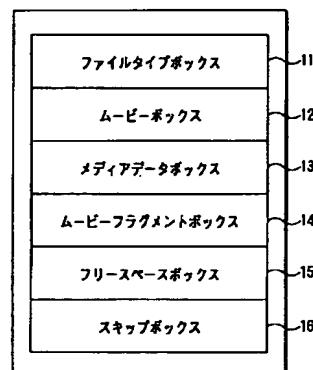
(54)【発明の名称】マルチメディア・ファイル・フォーマットのデータ構造、その暗号化方法並びに装置及びその暗号の復号化方法及び装置

## (57)【要約】

【課題】コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法を提供するにある。

【解決手段】マルチメディア・ファイル・フォーマットのデータ構造においては、ムービーボックス及びメディアデータボックスが設けられている。各ボックスは、非暗号化されたサイズ・フィールド及びタイプ・フィールド並びにボックス・データ・フィールドを備えている。ムービーボックスのボックス・データ・フィールドには、非暗号化或いは暗号化されたマルチメディア・データに関する情報データが格納され、メディアデータボックスのボックス・データ・フィールドには、暗号化されたマルチメディア・データが格納されている。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

当該第1のポックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のポックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のポックス・データ・フィールドを含む第1のポックスと、及び当該第2のポックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のポックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のポックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のポックス・データ・フィールドを含む第2のポックスと、

から構成されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 2】**

前記第1或いは第2のポックスは、前記第1及び第2のサイズ・フィールドが夫々所定の値を有するとき、夫々当該サイズ・フィールドと共に当該ポックスのサイズをバイトで示すための第1及び第2のロングサイズ・フィールド含むことを特徴とする請求項1のマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 3】**

前記第1のポックスでは、前記マルチメディア・データの音声或いは動画の符号化データがサンプル列として第1のポックス・データ・フィールドに格納され、当該サンプルは、暗号化符号化データを含むことを特徴とする請求項1のマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 4】**

前記第1のポックスでは、前記マルチメディア・データの音声或いは動画の符号化データがサンプル列として第1のポックス・データ・フィールドに格納され、1又は複数のサンプルがチャンクに定められ、当該チャンクは、暗号化符号化データを含むことを特徴とする請求項1のマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 5】**

前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャンク、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項3又は請求項4のいずれかに記載のマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 6】**

前記情報データが暗号化されて第2のポックス・データ・フィールドに格納されることを特徴とする請求項1のマルチメディア・ファイル・フォーマットのデータ構造。

**【請求項 7】**

第1のサイズ・フィールド、第1のタイプ・フィールド及び第1のポックス・データ・フィールドを含む第1のポックスと、及び第2のサイズ・フィールド、第2のタイプ・フィールド及び第2のポックス・データ・フィールドを有する第2のポックスとから構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する方法において、

前記マルチメディア・データを暗号化して第1のポックス・データ・フィールドに格納し、

前記第1のポックス・データ・フィールドに格納されたマルチメディア・データに関する情報データを第2のポックス・データ・フィールドに格納し、

夫々前記第1及び第2のポックスのサイズをバイトで示すための第1及び第2のサイズ情報を暗号化せずに前記第1及び第2のサイズ・フィールドに格納し、及び

夫々前記第1及び第2のポックスの種別を識別する第1及び第2のタイプ情報を記述する前記第1及び第2のタイプ・フィールドを暗号化せずに第1及び第2のポックスに格納

50

することを特徴とする暗号化方法。

【請求項 8】

前記マルチメディア・データの音声或いは動画の符号化データがデータ単位としてのサンプル列に分離され、このデータサンプルが暗号化されて前記第1のボックス・データ・フィールドに格納されていることを特徴とする請求項7の暗号化方法。

【請求項 9】

前記マルチメディア・データの音声或いは動画の符号化データがデータ単位としてのサンプル列に分離され、1又は複数のサンプルがチャunkに定められ、このチャunkが暗号化されて前記第1のボックス・データ・フィールドに格納されていることを特徴とする請求項7の暗号化方法。

10

【請求項 10】

前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャunk、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項8又は請求項9のいずれかに記載の暗号化方法。

【請求項 11】

前記情報データは暗号化されて第2のボックス・データ・フィールドに格納されることを特徴とする請求項7に記載の暗号化方法。

【請求項 12】

第1のサイズ・フィールド、第1のタイプ・フィールド及び第1のボックス・データ・フィールドを含む第1のボックスと、及び、第2のサイズ・フィールド、第2のタイプ・フィールド及び第2のボックス・データ・フィールドを有する第2のボックスと、から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する装置であって、

20

前記マルチメディア・データを暗号化して第1のボックス・データ・フィールドに格納する暗号化部と、

前記マルチメディア・データに関する情報データを第2のボックス・データ・フィールドに格納する第1の格納部と、

夫々第1及び第2のサイズ情報を暗号化せずに前記第1及び第2のサイズ・フィールドに格納する第2の格納部と、及び

30

前記第1及び第2のボックスの種別を識別する第1及び第2のタイプ・フィールドを夫々暗号化せずにに対応するボックスに格納する第3の格納部と、  
から構成されることを特徴とする暗号化装置。

【請求項 13】

前記暗号化部は、マルチメディア・データの音声或いは動画の符号化データをデータ単位としてのサンプル列に分離し、このデータサンプルを暗号化して前記第1のボックス・データ・フィールドに格納することを特徴とする請求項12の暗号化装置。

【請求項 14】

前記暗号化部は、前記マルチメディア・データの音声或いは動画の符号化データをデータ単位としてのサンプル列に分離し、1又は複数のサンプルをチャunkに定め、このチャunkを暗号化されて前記第1のボックス・データ・フィールドに格納することを特徴とする請求項12の暗号化装置。

40

【請求項 15】

前記暗号化部において、前記暗号化符号化データは、所定のデータ長として定められたブロックを単位とし暗号化されたデータ列であって、このブロックを基準として前記チャunk、或いは、前記サンプル内には、非暗号化符号化データ列を含むことを特徴とする請求項13又は請求項14のいずれかに記載の暗号化装置。

【請求項 16】

第1の格納部は、前記情報データを暗号化して第2のボックス・データ・フィールドに格納することを特徴とする請求項12に記載の暗号化装置。

50

**【請求項 17】**

当該第1のボックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のボックス・データ・フィールドを含む第1のボックスと、及び

当該第2のボックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のボックス・データ・フィールドを含む第2のボックスと、  
10

から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する方法において、

前記第2のボックスデータに格納されている情報データを獲得してこれを保持し、及びこの情報データを基にして前記第1のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力することを特徴とする暗号復号化方法。

**【請求項 18】**

当該第1のボックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のボックス・データ・フィールドを含む第1のボックスと、及び

20

当該第2のボックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のボックス・データ・フィールドを含む第2のボックスと、

から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する装置において、

前記2のボックスデータに格納されている情報データを獲得してこれを保持する獲得部と、及び

この情報データを基にして前記第1のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力する出力部と、  
30

を具備することを特徴とする暗号化装置。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

この発明は、マルチメディア・ファイル・フォーマットのデータ構造、その暗号化方法並びに装置及びその暗号の復号化方法及び装置に係り、特に、動画記録装置及び再生装置における動画ファイルの暗号化方法及びその装置に関する。

**【0002】****【従来の技術】**

近年、動画などのコンテンツは、アナログ・データからデジタル・データに移行しつつある。デジタル化されたコンテンツは、品質の劣化無しにコピーできるため、ユーザ間でCD-R、記録可能DVDディスク、或いは、メモリーカードを介して、又は、インターネット等の通信手段を利用したファイル転送技術、例えば、Eメールに添付してコンテンツ・データを送ってコンテンツ・データをコピーすることが可能となり、このようなコピーが横行しつつあり、コンテンツ業界で著作権上問題となっている。

40

**【0003】**

デジタルコンテンツの著作権を保護するための解決手段として、コンテンツデータに暗号をかける方法があり、この暗号化によって不正なコピーを防ぐことができる。従来のコンテンツデータに暗号をかける場合、一般にコンテンツデータの先頭から終端まで一括し  
50

て暗号化する方法がとられている。これにより、コンテンツデータを利用する権利があるもの、即ち、暗号を解く権限があり、その手段を有するもののみがコンテンツデータを利用することが可能となる。

#### 【0004】

##### 【発明が解決しようとする課題】

上述したような従来の暗号化方法においては、コンテンツデータを先頭から終端まで一括して暗号化する場合には、コンテンツデータの不正コピーを防ぐことはできる。しかしながら、コンテンツデータの先頭から終端まで一括して暗号化しているため、コンテンツデータの任意の位置にアクセスすることが容易でなく、任意の位置にアクセスする為には、アクセス対象とされていないデータであっても復号化して暗号化を解く必要があり、実質上、無駄な処理が要求される問題がある。即ち、従来、暗号化されたコンテンツデータの任意の位置にアクセスする際には、コンテンツの先頭から順次暗号を解き、所望のコンテンツの位置に到達するまで暗号を解く処理が必要とされる。このような処理は、アクセス位置のデータを獲得するまでに処理時間がかかる問題がある。

10

#### 【0005】

このように所望のコンテンツの位置に到達するまでの暗号を解く処理は、所望の位置をアクセスするためのみに必要とされる処理であって、実際にコンテンツデータを利用するため必要とされる処理ではないことから、無駄な処理ということができる。

#### 【0006】

所望するアクセス位置がファイルの先頭から離れれば離れるほど、上記の無駄な処理及び処理時間は増大する。処理負荷及び処理時間が増大するとそれに伴い消費電力も増大することになるので、バッテリを利用するポータブル機器などには連続使用時間が削減されるという問題もある。

20

#### 【0007】

コンテンツデータの任意の位置へのアクセスは、動画の再生においては、例えば、早送り再生、巻き戻し再生、ランダムアクセス再生、レジューム再生（ユーザが再生停止したところから、再度再生を再開する機能）を実現するときに必要とされる。

#### 【0008】

この発明は、上述した事情に鑑みなされたものであって、その目的は、コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法を提供するにある。

30

#### 【0009】

##### 【課題を解決するための手段】

この発明によれば、

当該第1のボックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のボックス・データ・フィールドを含む第1のボックスと、及び

当該第2のボックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のボックス・データ・フィールドを含む第2のボックスと、

40

から構成されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造が提供される。

#### 【0010】

また、この発明によれば、

第1のサイズ・フィールド、第1のタイプ・フィールド及び第1のボックス・データ・フィールドを含む第1のボックスと、及び第2のサイズ・フィールド、第2のタイプ・フィールド及び第2のボックス・データ・フィールドを有する第2のボックスとから構成され

50

るファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する方法について、

前記マルチメディア・データを暗号化して第1のボックス・データ・フィールドに格納し、

前記第1のボックス・データ・フィールドに格納されたマルチメディア・データに関する情報データを第2のボックス・データ・フィールドに格納し、

夫々前記第1及び第2のボックスのサイズをバイトで示すための第1及び第2のサイズ情報を暗号化せずに前記第1及び第2のサイズ・フィールドに格納し、及び

夫々前記第1及び第2のボックスの種別を識別する第1及び第2のタイプ情報を記述する前記第1及び第2のタイプ・フィールドを暗号化せずに第1及び第2のボックスに格納することを特徴とする暗号化方法が提供される。  
10

### 【0011】

更に、この発明によれば、

第1のサイズ・フィールド、第1のタイプ・フィールド及び第1のボックス・データ・フィールドを含む第1のボックスと、及び、第2のサイズ・フィールド、第2のタイプ・フィールド及び第2のボックス・データ・フィールドを有する第2のボックスと、から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを暗号化する装置であって、

前記マルチメディア・データを暗号化して第1のボックス・データ・フィールドに格納する暗号化部と、  
20

前記マルチメディア・データに関する情報データを第2のボックス・データ・フィールドに格納する第1の格納部と、

夫々第1及び第2のサイズ情報を暗号化せずに前記第1及び第2のサイズ・フィールドに格納する第2の格納部と、及び

前記第1及び第2のボックスの種別を識別する第1及び第2のタイプ・フィールドを夫々暗号化せずにに対応するボックスに格納する第3の格納部と、  
から構成されることを特徴とする暗号化装置が提供される。

### 【0012】

更にまた、この発明によれば、

当該第1のボックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のボックス・データ・フィールドを含む第1のボックスと、及び

当該第2のボックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のボックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のボックス・データ・フィールドを含む第2のボックスと、

から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する方法において、  
40

前記第2のボックスデータに格納されている情報データを獲得してこれを保持し、及びこの情報データを基にして前記第1のボックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力することを特徴とする暗号復号化方法が提供される。

### 【0013】

また更に、この発明によれば、

当該第1のボックスのサイズをバイトで示すための第1の非暗号化サイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別する第1の非暗号化タイプ情報を格納する第1のタイプ・フィールド及び暗号化されたマルチメディア・データを格納する第1のボックス・データ・フィールドを含む第1のボックスと、及び  
50

当該第2のポックスのサイズをバイトで示すための第2の非暗号化サイズ情報を格納する第2のサイズ・フィールド、当該第2のポックスの種別を識別する第2の非暗号化タイプ情報を格納する第2のタイプ・フィールド及び前記第2のポックスデータに格納されたマルチメディア・データに関する情報データを格納する第2のポックス・データ・フィールドを含む第2のポックスと、

から構成されるファイル・フォーマット構造を有するマルチメディア・ファイルを復号化する装置において、

前記2のポックスデータに格納されている情報データを獲得してこれを保持する獲得部と、及び

この情報データを基にして前記第1のポックスデータに格納されたマルチメディア・データの少なくとも一部を暗号復号化して出力する出力部と、  
10  
を具備することを特徴とする暗号化装置が提供される。

【0014】

【発明の実施の形態】

以下、図面を参照しながらこの発明の暗号化方法の一実施例について説明する。

【0015】

この発明の暗号化方法がMPEG-4ファイル・フォーマットに適用される実施例について図1から図18を参照して説明する。

【0016】

図1は、ISOにて規格化されているMPEG-4ファイル・フォーマット(FILE FORMAT)の構造を示している。以下の説明において、MPEG-4ファイル・フォーマットは、単にMP4と省略して説明する。MP4は、MPEG-4に従って符号化されたビデオストリーム、或いは、オーディオストリームを格納するためのファイル・フォーマットである。このファイル・フォーマットには、定義により、MPEG-4以外のコーデックも格納することが可能である。尚、このMP4データは、ファイルとしてディスク上に格納されている場合、或いは、バイナリイメージとしてメモリ上に格納されている場合等が想定される。

20

【0017】

図1に示すように、MP4は、オブジェクト構造を有し、幾つかのポックスより構成されている。このポックスは、文献によりアトム(atom)と称せられる場合があることに注意されたい。MP4では、ポックス中に、さらにポックスを入れた入れ子状態で格納することができるとされている。ここで、入れ子状態、即ち、階層構造になっているポックスの最初のポックス、即ち、最上位のポックスは、トップレベルポックスと称せられる。図1には、トップレベルポックスのみが示されている。

30

【0018】

図1に示すように、トップレベルポックスは、幾つかの種類がある。即ち、MP4ファイルは、ファイルタイプポックス11、ムービーポックス12、メディアデータポックス13、ムービーフラグメントポックス14、フリースペースポックス15及びスキップポックス16等から構成される。これらのポックスは、MP4ファイル中に必須のもの、或いは、オプションで記述されれば良いものがある。

40

【0019】

MP4では、これらのポックスは、図1に示すような順序で配列されることは要求されず、前述したような規定項目の範囲内で構成を変更することが可能である。しかし、ここでは、特に具体的な規定内容については説明を省略する。ただし、ポックスによって出現個数、位置、有無が規定され、データによりトップレベルポックスの構成が異なることがMP4の特徴であるとされている。

【0020】

ここで、各トップレベルポックスの機能について説明する。ファイルタイプポックス11は、ファイルのブランド或いはバージョン等のファイルのタイプを格納するポックスであり、MP4で定まったファイルであることを記述している。ムービーポックス12は、M  
50

P 4 データ全体のメタデータ、つまり符号化されたメディアのコーデックストリームをデコードするために必要な情報等、例えば、データのデコードに必要とされる属性及びアドレス等が記述されている情報を格納している。メディアデータボックス 1 3 は、実際の符号化されたメディアのコーデックストリーム、即ち、ビデオストリーム、或いは、オーディオストリーム等のコンテンツデータを格納している。ムービーフラグメントボックス 1 4 は、ムービーボックス 1 2 の情報を分割して格納するためのボックスである。フリースペースボックス 1 5 及びスキップボックス 1 6 は、ユーザーデータや、パディングのためにパディングデータを格納するためのボックスである。ユーザーデータボックス 1 7 は、ユーザが定めたデータが格納されるボックスである。

#### 【0021】

次に、ボックスの構造について説明する。ボックスは、全てのボックスにおいて共通の構造を有している。図 2 には、共通の構造を有するボックス 2 0 を示している。このボックス 2 0 においては、先頭の 4 バイトがボックスのサイズをバイトで示すためのサイズ・フィールド 2 1 に定められている。次の、4 バイトは、ボックスの種別を識別するタイプ・フィールド 2 2 に定められている。ボックスの種別は、4 つのキャラクターにより識別され、例えば、ムービーボックス 1 2 の場合は ‘m o o v’ となり、ムービーデータボックスの場合は ‘m d a t’ となる。この 4 文字のキャラクターをマッチングさせることによりボックスの種別を識別することが可能となる。次に、タイプ・フィールド 2 2 に続いてボックス・データ・フィールド 2 3 が格納されている。このボックス・データ・フィールドの構造は、各ボックスにおいて用途によりシンタックスが定義されている。このボックス・データ・フィールドのサイズは、サイズ・フィールド 2 1 の値からサイズ・フィールド 2 1 とタイプ・フィールド 2 2 で用いられている 8 を除いた値となる。

10

#### 【0022】

図 3 に示すように、サイズ・フィールドの値が 1 のときは (size == 1) 、このボックス 2 0 では、タイプ・フィールド 2 2 とボックス・データ・フィールド 2 3 の間に当該サイズ・フィールド 2 4 とともにボックスのサイズを示す 8 バイトのラージサイズ・フィールド 2 4 が出現し、ボックスのサイズが 4 バイトのサイズ・フィールド 2 1 で表現できないような大容量のボックスにも対応できるようになっている。このボックス 2 0 では、ボックス・データ・フィールド 2 3 のサイズは、ラージサイズ・フィールドに格納されているサイズから 1 6 を除いた値となる。

20

#### 【0023】

この発明の一実施例に係る暗号化方法においては、トップレベルのボックス毎にデータが暗号化及び非暗号化が決定される。即ち、図 4 に示すようにサイズ・フィールド 2 4 の値が 1 でない場合 (size != 1) のサイズ・フィールド及びタイプ・フィールドのデータは、暗号化されず（以下、単に暗号化されていない場合は、非暗号化と称する場合がある。）、ボックスデータが暗号化の対象とされている。

30

#### 【0024】

尚、メディアデータボックス 1 3 のメディアデータは、後に述べるように暗号化されことが必須とされる。他のボックス 1 1 、 1 2 、 1 4 ～ 1 6 のボックスデータは、後に述べるように暗号化されても良く或いはされなくとも良い。

40

#### 【0025】

図 5 に示されるように、サイズ・フィールド 2 4 の値が 1 で、タイプ・フィールド 2 2 とボックスデータ部 2 3 の間にラージサイズ・フィールド 2 4 がある場合にあっても、このラージサイズ・フィールド 2 4 も暗号化の対象とされない。暗号化の方法によっては、データのブロック長が複数バイト必要な場合がある。即ち、暗号化の対象とされるデータが所定のブロック長で分割されてデータが暗号化される場合には、所定のブロック長未満の残余のデータが生じ、このデータ長が暗号化に必要とされるバイト数に達しない虞がある。このように暗号化されるデータ中で残余のバイトが生じ、このバイト数が暗号化の対象バイト数よりも小さい場合には、図 6 に示されるように、この残余のブロック中の残余のデータに対しては、暗号化しないようにしても良い。一例としては、ボックスデータ長が

50

15バイトで、暗号手法がデータのブロック長を8バイト必要とする場合が該当する。この場合、ボックスデータの最初の8バイトは、暗号化され、残りの7バイトは暗号化されないこととなる。

【0026】

以上のように、ボックスデータ部に対してデータを暗号化することで、例えば、ムービーボックス12にアクセスが試みられた際に、始めに、MP4データの先頭の8バイトが取得されてボックスサイズ及びボックスタイプ・フィールドが獲得される。次に、ボックスタイプがムービーボックス12のタイプと一致するかが確認される。一致しない場合、即ち、ボックスタイプがムービーボックス12のタイプでない場合には、アクセスointerがボックスサイズ分だけずらされ、次の8バイトが取得されてボックスサイズとボックスタイプ・フィールドが獲得される。ボックスタイプがムービーボックス12のタイプと一致するまでこのアクセスointerのシフトが繰り返えされる。ボックスタイプがムービーボックス12のタイプと一致すると、暗号化されているボックスデータは、順次その暗号化が解れてムービーボックス12中のボックスデータへアクセスすることが可能となる。

10

【0027】

次に、メディアデータボックス13中のメディアデータは、暗号化される場合について説明する。

【0028】

メディアデータボックス13は、他のトップレベルボックスがメディアストリームのデコードに必要な情報を格納しているのと異なり、メディアデータが格納されている。このメディアデータの暗号化に際しては、スキップ再生、早送り再生、巻き戻し再生、或いは、レジューム再生等の特殊再生時に、メディアデータの任意の位置に効率よくアクセスすることができる必要とされる。そのために、図6に示すように、上述のサイズ・フィールド及びタイプ・フィールドを暗号化しないことに加え、ストリームデータは、独立した符号化単位毎に暗号化がなされる。ここでは、符号化単位とは、音声ストリームに関しては、サンプル、若しくは、フレームが相当し、動画ストリームに関しては、フレームが相当する。

20

【0029】

この発明に実施例に係るメディアデータボックス13内のメディアデータの暗号化では、暗号化される符号化の単位は、MP4データ内のサンプルが対象とされる。サンプルに代えて、チャンクがメディアデータボックス13内で暗号化されても良い。各サンプルについてのMP4データ内での位置は、そのサンプルについて記述するムービーボックス12のチャンクオフセット及びサンプルサイズを解析することによって得ることができる。即ち、サンプルが属するチャンクの位置は、データファイル先頭からのオフセットとしてチャンクオフセットに記述され、そのチャンクに含まれるサンプルについては、そのサイズがサンプルサイズに記述されている。従って、何れのサンプルもチャンクオフセット及びサンプルサイズを参照することによって、そのオフセットを求めることができる。

30

【0030】

ここで、より説明を明確にする為にMP4におけるムービーボックス12の構造及びメディアデータボックス13内のデータ構造を図8から図10を参照して説明する。

40

【0031】

図8は、m o o v (Movie Box)と称せられるムービーボックス12の構造を示している。この図8に示されるボックスには、図4から図8を参照して説明した暗号化の対象とされないサイズ・フィールド、ラージサイズ・フィールド及びタイプ・フィールドは、図示されず、データボックス部に相当するムービーボックス12(ムービーボックス:Movie Box)のみが示されている。同様に図8には、メディアデータボックス13としてm d a t (メディアデータボックス13:Media Data Box)が示されているが、この内には、サイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドがあり、ボックスデータとして実データとしてのコンテンツデータ(マルチメディア・データ)が格納されている。図8及び図9A及び9Bを参照する

50

説明においては、サイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドがあるものとして説明を理解されたい。

【0032】

この図8に示されるフォーマットでは、1つのMP4ファイルは、第1階層のヘッダとしてファイル情報が記載されるmoov (ムービーボックス: Movie Box) 及び音声データ及び映像データを含むマルチメディア・データが格納されているmdat (メディアデータボックス13: Media Data Box) から構成されている。このMP4ファイルには、付加的に、第1階層の空き領域としてのfree (フリー) 並びにskip (スキップ) 及びユーザが定義する書き込みを許すudta (ユーザデータボックス: User Data Box) が設けられている。

10

【0033】

尚、MP4ファイルでは、一般にボックス (box) と称される単位を元にデータを分類し、管理されている。このボックス (box) は、上位層から下位層に至る階層構造を取ることができ、その内部に更に下位層のボックス (box) を含むものを「コンテナボックス」と称している。ここで説明するボックスは、アトム (atom) と称される場合がある。

【0034】

また、ヘッダとしてのmoov (Movie Box) には、第2階層にあるMP4ファイルの作成時刻及びMP4ファイルのコンテンツ長等のヘッダ情報が記述されているmvhd (ムービーヘッダボックス: Movie Header Box) 、オブジェクト、即ち、再生対象に関する情報が記述されているiods (オブジェクトディスクリプタボックス: Object descriptor Box) 及び多重化されているメディア情報に関する各種パラメータが記述されているtrak (トラック: Track Box) を含んでいる。このtrak (Track Box) は、多重化されているメディアが多数あれば、そのメディアの数だけ用意される。例えば、音声と映像とが多重化されたコンテンツにあっては、音声メディアトラック及び映像メディアのトラックが用意され、その音声用のトラックに音声メディアのパラメータが格納され、映像用のトラックに映像メディアのパラメータが格納される。

20

【0035】

図8に示されるようにトラック (Track Box) は、第3階層にあるトラックの作成時刻及びトラックID (識別子) と称されるトラックを識別するための一連の番号が格納されているtkhd (トラックヘッダボックス: Track Header Box) 、トラックに関して記述されたtref (トラックリファレンスボックス: Track Reference Box) 、編集情報に関してのedts (エデットボックス: Edit Box) 及びメディアの情報に関して記述されたmdia (メディアボックス: Media Box) を含んでいる。エデットボックスedtsは、第4階層に編集リスト情報が記述されたelst (エデットリスト: ボックスEdit List Box) を含み、メディアボックスmdiaは、第4階層にこのメディアトラックのタイムスケール等の情報が格納されるmdhd (メディアヘッダ: Media Header) 、ヘッダを参照する情報が記述されたhdlr (ヘッダリファレンスボックス: Handler Reference Box) 及びメディアに関する情報が格納されているminf (メディアインフォメーションボックス: Media information Box) を含んでいる。メディアインフォメーションminfは、更に第5階層にトラックに格納されているメディアが映像であることを示すvmhd (ビデオメディアヘッダボックス: Video Media Header Box) 、或いは、トラックに格納されているメディアが音声であることを示すsmhd (サウンドメディアヘッダボックス: Sound Media Header Box) 、ヒント・メディアのヘッダ情報が記述されたhmhd (ヒントメディアヘッダボックス: Hint Media Header Box) 、メディアがビデオ或いは音声以外のMPEG-4ストリームである場合に、MPEG-4のヘッダ情報が記述されたmpeg (MPEG-4メディアボックス:

40

50

MPEG-4 Media Box)、メディア情報が記述されたminf (メディアインフォメーションボックス: Media Information Box) 及びサンプルに関する情報が記述されたstbl (サンプルテーブルボックス: Sample Table Box) を含んでいる。ビデオメディアヘッダボックスvmdat及びサウンドメディアヘッダボックスsmhdは、トラックに格納されているメディア、即ち、音声か映像化の種別に応じて逐一的に記載される。更にまた、dinf (データインフォメーションボックス: Data Information Box) は、データを参照する情報が記述されたdref (データリファレンスボックス: Data Reference Box) を含み、また、stbl (サンプルテーブルボックス: Sample Table Box) は、各サンプルのデコード時刻が設定されているstts (デコーディングタイム: Decoding time to Sample Box)、サンプルに対する表示。時間が記述されたctts (コンポジションタイム: Composition Time to Sample Box)、サンプルの同期情報が記述されたstss (シンクロサンプルボックス: Sync Sample Box)、コーディックの種別やデコードに必要となる各種情報が設定されているstsd (サンプルディスクリプションボックス: Sample Description Box)、トラック中のサンプルの総数 (サンプルカウント: sample\_count) 及び各サンプルのデータサイズ (エントリーサイズ: entry\_size) が設定されているstsz (サンプルサイズボックス: Sample Size Box)、チャンク内のサンプル数 (チャンクに対するサンプル: sample\_per\_chunk) 及びサンプルのインデックス (サンプルディスクリプションインデックス: sample\_description\_index) が記述されたstsc (チャンクに対するサンプル: Sample to Chunk Box)、チャンクに関するファイルの先頭からのオフセット位置情報 (チャンクオフセット: chunk\_offset) が記述されるstco (チャンクオフセットボックス: Chunk Offset Box)、同期情報が記述されたstsh (シャドウシンクサンプルボックス: Shadow Sync Sample Box) 及びstdp (デグラデーションプライオリティボックス: DegradationPriority Box) を含んでいる。stsd (Sample Description Box) は、必要に応じて複数個設定することができる。

**【0036】**  
ここで、図10に示すようにサンプル (即ち、sample) とは、映像や音声の実際のメディアデータをある大きさに区切った単位を称し、メディアデータは、このサンプルを基に管理されている。チャンク (即ち、chunk) は、1又は複数のサンプルが連接されているものを称し、ファイル先頭からのチャンクの位置や当該チャンクにいくつのサンプルが含まれているかと言った、データ領域の内部構造に関する情報は、上述したようにmoovコンテナボックスの下位階層に記述される。また、既に説明したように実際のメディアデータは、mdatボックスに配置され、音声や映像といったメディア毎の情報管理にトラックというボックスが割り当てられている。このようにMP4ファイルは、moovコンテナボックスを取得すれば、構成されるメディア数、それぞれの種別、データサイズ等が判明する。

**【0037】**  
尚、一般にMP4のボックスは、同一階層の配置順序の規定がない。図8の第1階層においては、moov、mdat、moof、free、skip、udtaの順序で並んでいるが、これは必ずしも規格上ファイル先頭からこの順番で並ばなければならないことを意味していない。例えば、図9Aに示すようにmdat、moov、free、skip、udtaの順序で並んでも良く、或いは、図9Bに示すようにmoov、udta、mdat、moof、mdat、skip、freeの順序で並んでも良い。更に、MP4ファイルでは、1つのmoovに対して複数のmdat、moofが設けられても良い。

**【0038】**  
図8に示したサイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フ

10

20

30

40

50

フィールドを除くm o o vコンテナボックス内のデータ暗号化され、また、同様にサイズ・フィールド並びにタイプ・フィールド、更には、ラージサイズ・フィールドを除くm d a tコンテナボックス内の実データが暗号化される。

#### 【0039】

この暗号化は、一例として図11に示すような動画像記録システム100で実現され、この動画像記録システム100において、音声及び映像データが図12に示すような手順で暗号化される。この動画像記録システム100における暗号化を含むフォーマットの手順についてこの図11及び図12を参照して説明する。

#### 【0040】

マイク101或いはオーディオ入力装置から取り込まれたオーディオ信号は、オーディオエンコーダ102でエンコードされて符号化オーディオデータ、例えば、MP4オーディオデータに変換される。同様に、カメラ103或いは映像入力装置から取り込まれたオーディオ信号は、ビデオエンコーダ104でエンコードされて符号化ビデオデータ、例えば、MP4ビデオデータに変換される。ここで、外部入力装置としてのマイク101、カメラ103からは、アナログ信号でも、或いは、デジタル信号の何れで動画像記録システム100に入力されても良い。オーディオエンコーダ102からは、その内で生成された音声符号化ストリームがファイル生成部105へ出力され、ビデオエンコーダ104からは、同様に、その内で生成されたビデオ符号化ストリームがファイル生成部105へ出力される。ファイル生成部105では、オーディオエンコーダ102及びビデオエンコーダ104から出力された音声符号化ストリーム及びビデオ符号化ストリームが図8に示すような所定のMP4ファイル・フォーマット形式に整えられ、ローカルメモリ106上に展開される。このファイル生成の完了後、図12及び図13を参照して説明するように暗号化部107がローカルメモリ106に蓄積されているファイルを所定の暗号化方法で暗号化し、再度ローカルメモリ106に配置し、暗号化ファイルとして出力する。

#### 【0041】

暗号化が開始されると（ステップS10）、ステップS11に示されるようにローカルメモリ106上へ展開されたMP4ファイルからムービーボックス12（m o o v）が検索される。ここで、ムービーボックス12は、トップレベルボックスであるので、ファイルの先頭からサイズ・フィールド及びタイプ・フィールドを読み出し、タイプ・フィールドがm o o vと示されているものが検索される。最初のボックスがm o o vではない場合には、読み出したサイズ分だけファイル中でシークされ、次のボックスが解析される。タイプ・フィールドがm o o vとの表示があるまで検索が継続される。

#### 【0042】

ムービーボックス12が検出されると、ムービーボックス12中に格納されているトラック毎のチャンクオフセットボックス（s t c o）及びサンプルトゥチャンクボックス（s t s c）、サンプルサイズボックス（s t s z）が検索され、それらに保持されているテーブルがメモリ上に保持される。即ち、ステップS12において、Nの初期値は1に設定され、このムービーボックス12内の最初のトラックtrack内に記述された最初のチャンクのチャンクオフセットs t c oが読み出され、このチャンクオフセットs t c o内のc h u n k \_ o f f s e tからそのオフセットアドレスが読み出されると共にサンプルサイズボックスs t s zのe n t r y \_ s i z eからそのトラックに属する全てのサンプルサイズが読み出される。また、チャンクオフセットs t c o内のe n t r y \_ c o u n tからそのトラック内の全てのチャンク数が読み出され、また、チャンクボックスに対するサンプルを意味するs t s cのs a m p l e \_ p e r \_ c h u n kから各チャンクのサンプル数が読み出され、サンプルサイズボックスs t s zのs a m p l e \_ c o u n tからそのトラック内の全てのサンプル総数が読み出される。

#### 【0043】

同様に他のトラックについて、同様の項目が読み出される。これらの読み出された項目からオフセットの順序でチャンク毎のオフセット及びサンプル毎のオフセットが記述されたテーブルが作成される。

10

20

30

40

50

## 【0044】

即ち、図10に示すようにオーディオトラックに属するオーディオチャンク (A chunk) 及びビデオトラックに属するビデオチャンク (V chunk) が交互に表れるようなメディアデータボックス13に格納されているメディアデータでは、オフセット0からオフセットxで示されるチャンクに関するテーブルが作成され、各チャンクに関するオフセットアドレスが chunk\_of\_fset からそのテーブルにコピーされる。また、そのテーブルには、各チャンクを構成するサンプル数に応じてサンプルの項目が作成され、該当するサンプルのサンプルサイズからそのサンプルの位置及びそのサイズが記述される。作成されたテーブルにおいて、チャンクの総数及びサンプルの総数は、各トラックのチャンク数及びサンプル数でその総数が確認される。

10

## 【0045】

次に、このテーブルが参照されてステップS13に示すようにメディアデータボックス13内の最初のサンプルが暗号化されてローカルメモリ106に書き込まれる。次に、暗号化されたサンプルの番号NがステップS13においてメディアデータボックス13内の最後のサンプルかが確認される。暗号化されたサンプルが最後のサンプルでない場合には、ステップS14に示されるように暗号化されるべきサンプル番号が1つ増加され、再びステップS12に示すようにテーブルからサンプルの位置及びサイズを取得するステップに戻され、ステップS13において、その該当サンプルが暗号化される。ステップS12からステップS15が繰り返されてステップS15において暗号化されたサンプルがメディアデータボックス (mdat) 13内の最後のサンプルに相当する場合には、その処理が 20  
ステップS18に示すように終了される。

## 【0046】

メディアデータボックス (mdat) 13以外の他のボックスが暗号化される場合には、図13に示すように図12と同様にステップS11からステップS15が実行される。ステップS15において暗号化されたサンプルがメディアデータボックス (mdat) 13内の最後のサンプルに相当する場合には、メディアデータボックス13内の実データの暗号化が終了されたとして他のボックスがステップS16で暗号化される。例えば、メディアデータボックス13内の実データの暗号化するために利用されたムービーボックス12 (mov) が暗号化される。当然ながら、既に説明したようにメディアデータボックス13及びムービーボックス12 (mov) 内のサイズ・フィールド、タイプ・フィールド、更には、ラージサイズ・フィールドは、何れも暗号化されない。

30

## 【0047】

ステップS17において、全てのボックスが暗号化されていない場合には、再びステップS16に戻されて次々にMP4ファイル内のボックスが暗号化される。

## 【0048】

ステップS17において、全てのボックスの暗号化が終了すると、その処理がステップS18に示すように終了される。

## 【0049】

上述した説明において、メディアデータボックス13では、既に説明したようにサンプルが所定のブロック長毎に暗号化され、残余の部分が生じた場合には、その部分は暗号化されないこととなる。例えば、所定のブロック長が8バイトであり、サンプルがこの8バイトの整数 (n) 倍のサイズNバイト ( $N = n \times 8$ ) を有する場合には、図14に示すようにそのサンプルは、非暗号化の残余なしで暗号化される。これに対して、所定のブロック長が8バイトであり、サンプルがこの8バイトの整数 (n) 倍のサイズを超えるバイト ( $N = n \times 8 + m$ 、但し、 $m < 8$ ) を有する場合には、図15に示すようにそのサンプルの所定のブロック長部分8バイトの整数倍の部分 ( $n \times 8$  ビット) は、暗号化され、残余の部分 ( $m$  バイト) は、暗号化されない。同様に、所定のブロック長が8バイトであり、サンプルがこの8バイトの整数 (n) 倍のサイズ以内のバイト ( $N < 8$ ) を有する場合には、図16に示すようにそのサンプルは、暗号化されないこととなる。

40

## 【0050】

50

尚、図13を参照して説明した暗号化処理では、前提として、ローカルメモリ106上にMP4ファイルが蓄積されていることを想定しているが、即ち、ファイルの生成は、完了しているものとしている。しかしながら、ファイルが生成されながらの暗号化処理が実施されても良いことは明らかである。

#### 【0051】

この暗号化された音声及び映像データを含むファイルは、一例として図17に示すような動画像再生システム100で復号化される。この動画像記録システム100における復号化は、図18に示すような手順で実現される。この動画像記録システム100における復号化の手順についてこの図17及び図18を参照して説明する。

#### 【0052】

図17は、MP4ファイルの暗号化された音声及び映像データを復号化して音声及び映像信号に変換する動画像再生システム200を示している。この動画像再生システム200においては、図13に示した暗号化処理が施されたMP4ファイルがローカルメモリ206に入力され、このローカルメモリ206に格納される。図18を参照して説明するよう暗号化されたファイルは、暗号復号化部207にて所定の暗号復号方法で暗号が復号され、再度、ローカルメモリ206に配置される。このローカルメモリに展開されたファイルがファイル解析部205において音声符号化ストリーム及びビデオ符号化ストリームに分離され、それぞれオーディオデコーダ202及びビデオデコーダ204に供給される。オーディオデコーダ202は、供給された音声符号化ストリームをデコードして音声信号をスピーカ201に出力して再生させている。また、ビデオデコーダ204は、供給されたビデオ符号化ストリームをデコードしてビデオ信号を画像出力装置203に出力し、動画像を画像出力装置203に表示させている。

10

20

30

#### 【0053】

図18を参照して暗号化されたファイルを復号する為の手順を説明する。ここでは、前提として、ローカルメモリ206上には、暗号化されたMP4ファイルが蓄積され、また、メディアデータボックス13内では、サンプル毎に暗号化されているものとする。

#### 【0054】

暗号の復号化処理が開始されると（ステップS20）、メディアデータボックス（m d a t）13を除く他のボックスについて、ステップS21に示すように暗号の復号化処理が実施される。図4から図7を参照して既に説明したように各ボックスにおいては、サイズ・フィールド、タイプ・フィールド、更には、ラージサイズ・フィールドは、何れも暗号化されていないことから、これらのフィールドが参照されてメディアデータボックス（m d a t）13以外のボックスかが確認され、各ボックスの暗号化されたボックスデータ部が復号化される。復号化されたボックスは、再びローカルメモリ206上に蓄積される。ステップS22に示すようにメディアデータボックス（m d a t）13以外のボックスの復号化処理が終了するまで繰り返され、この処理が終了すると、ステップS23で示す次の処理へ移行される。

40

#### 【0055】

メディアデータボックス（m d a t）13のみが暗号化され、他のボックスが暗号化されていない場合には、スタートS20後ステップS23に示す処理が実施される。

40

#### 【0056】

ステップS23においては、復号化処理が施されたムービーボックス12がファイル中から検索される。ムービーボックス12が検索されると、ステップS24に示すように暗号化時と同様の方法でムービーボックス12中に格納されているトラック毎のチャンクオフセットボックス（s t c o）及びサンプルトゥチャンクボックス（s t s c）、サンプルサイズボックス（s t s z）が検索され、それらに保持されているテーブルがメモリ上に保持される。即ち、ステップS12において、Nの初期値は1に設定され、このムービーボックス12内の最初のトラックt r a c k内に記述された最初のチャンクのチャンクオフセットs t c oが読み出され、このチャンクオフセットs t c o内のc h u n k\_o f f s e tからそのオフセットアドレスが読み出されると共にサンプルサイズボックスs t s

50

`z` の `entry_size` からそのトラックに属する全てのサンプルサイズが読み出される。また、チャンクオフセット `stco` 内の `entry_count` からそのトラック内の全てのチャンク数が読み出され、また、チャンクボックスに対するサンプルを意味する `stsc` の `sample_per_chunk` から各チャンクのサンプル数が読み出され、サンプルサイズボックス `stsz` の `sample_count` からそのトラック内の全てのサンプル総数が読み出される。

#### 【0057】

同様に他のトラックについて、同様の項目が読み出される。これらの読み出された項目からオフセットの順序でチャンク毎のオフセット及びサンプル毎のオフセットが記述されたテーブルが作成される。

10

#### 【0058】

即ち、図10に示すようにオーディオトラックに属するオーディオチャンク (`A chunk`) 及びビデオトラックに属するビデオチャンク (`V chunk`) が交互に表れるようなメディアデータボックス13に格納されているメディアデータでは、オフセット0からオフセット `x` で示されるチャンクに関するテーブルが作成され、各チャンクに関するオフセットアドレスが `chunk_of_offset` からそのテーブルにコピーされる。また、そのテーブルには、各チャンクを構成するサンプル数に応じてサンプルの項目が作成され、該当するサンプルのサンプルサイズからそのサンプルの位置及びそのサイズが記述される。作成されたテーブルにおいて、チャンクの総数及びサンプルの総数は、各トラックのチャンク数及びサンプル数でその総数が確認される。

20

#### 【0059】

次に、このテーブルが参照されてステップS25に示すように最初のサンプルが復号化されてローカルメモリ106に書き込まれる。次に、復号化されたサンプルの番号 `N` がステップS13においてメディアデータボックス13内の最後のサンプルかが確認される。復号化されたサンプルが最後のサンプルでない場合には、ステップS27に示されるように復号化されるべきサンプル番号が1つ増加され、再びステップS24に示すようにテーブルからサンプルの位置及びサイズを取得するステップに戻され、ステップS25において、その該当サンプルが復号化される。ステップS24からステップS27が繰り返されて暗号化されたサンプルがメディアデータボックス (`mdat`) 13内の最後のサンプルに相当する場合には、メディアデータボックス13内の実データの復号化が終了される。

30

#### 【0060】

上述した実施例の変形例として、ムービーフラグメントボックスを参照して各サンプルのオフセットを獲得しても良い。即ち、ムービーフラグメントボックスがあるMP4ファイルでは、ムービーフラグメントボックスにチャンクオフセット `stco` 及びサンプルサイズ `stsz` が記述されている。従って、このチャンクオフセット `stco` 及びサンプルサイズ `stsz` を解析することによって同様に各サンプルのオフセットを獲得することができる。

#### 【0061】

上述した実施例においては、このサンプルのオフセット値及びサイズを用いてサンプル内のデータが暗号化されている。サンプルは、符号化ストリームのデコードに必要な最小の単位のため、サンプル単位にアクセスすることができれば、前述の特殊再生において、任意の位置のサンプルを効率的にアクセスすることができる。即ち、図13に示す処理において、ステップS10からステップS12が実施され、ステップS12において、`N` 番目のサンプルが目的とされるサンプルであれば、その目的とされるサンプルのみが復号化され、この復号化されたサンプルが音声或いは映像信号にデコードされて再生される。この目的とされるサンプルのみの再生によって、動画の再生においては、例えば、早送り再生、巻き戻し再生、ランダムアクセス再生、ユーザが再生停止したところから、再度再生を再開するレジューム再生が実現される。音声の再生においても同様に再生可能となる。

40

#### 【0062】

50

尚、上述した実施例においては、メディアデータボックス13内では、サンプル毎に暗号化されている。このサンプル毎の暗号化に代えて、チャンク毎にチャンク内のデータが暗号化されても良い。既に説明したように、チャンクは、メディアデータ内の同一メディアのサンプルが連続している時の集合を示している。上記のサンプル単位毎に暗号化を行う場合と同様にチャンク毎に暗号化されれば良い。このチャンク毎の暗号化では、サンプル毎の暗号化に比べて、暗号化のリセットの回数が削減されるため、暗号化及び暗号を解く処理を軽減することが可能となる。尚、チャンク毎の暗号化及び復号化については、図13及び図18において、収集されるチャンクの情報を処理することによってサンプルと同様にチャンクの暗号化及び復号化が可能となる。

## 【0063】

10

この発明の暗号化方法及び復号化方法は、MP4ファイル・フォーマットを格納する機器、例えば、携帯電話、デジタルカメラ、デジタルムービー、デジタルハードディスクレコーダー、PDA等に適用することができる。

## 【0064】

また、同様のボックス構造を用いているJPEG2000のファイル・フォーマットにあっても、この発明の暗号化方法及び復号化方法を適用することができる。

## 【0065】

20

以上のように、この発明の実施例によれば、ボックス毎に暗号化を行うことによって、MP4データ内に存在する任意のボックスに効率的にアクセスすることが可能となる。さらに、サイズ・フィールド、タイプ・フィールド以外を暗号化することにより、平文であるサイズ・フィールド、タイプ・フィールドを用いて暗号を解く処理を行わずに所望のボックスへアクセスすることができる。

## 【0066】

また、この発明の実施例によれば、音声或いは動画の符号化データを含むボックスにアクセスすることができ、また、そのボックス内のサンプル或いはチャンクに効率的にアクセスすることができ、音声或いは動画の特殊再生が実現することが可能となる。

## 【0067】

30

## 【発明の効果】

以上のように、この発明によれば、コンテンツデータの所定の位置に効率的にアクセス可能なマルチメディア・ファイル・フォーマットのデータ構造及びその暗号化方法並びに暗号の復号化方法が提供される。

## 【図面の簡単な説明】

【図1】図1は、この発明の一実施例に係る暗号化方法が適用されるMP4ファイルの構造を概略的に示す平面図である。

【図2】図1に示される各ボックスの一般的な構造を概略的に示す平面図である。

【図3】図2に示した構造とは異なる他のタイプに係るボックスの構造を概略的に示す平面図である。

【図4】図1に示されるメディアデータボックス以外の他のトップレベルボックスに対する暗号化を説明する為の平面図である。

【図5】図2に示した構造とは異なる他のタイプに係るメディアデータボックス以外の他のトップレベルボックスに対する暗号化を説明する為の平面図である。

【図6】図4に示されるボックスに対する暗号化においてブロック単位で暗号化を施し、残余のデータが生じた際にその残余データに対しては暗号化を施さないことを説明する為の平面図である。

【図7】図1に示されるメディアデータボックスのヘッダの構造及びその非暗号化を示す平面図である。

【図8】図1に示されるムービーボックスの構造を示す平面図である。

【図9】(a)及び(b)は、図1に示されるムービーボックスの他の構造を示す平面図である。

【図10】図1に示されるメディアデータボックス内のデータ構造を説明する為の平面図 50

である。

【図11】この発明の一実施例に係る暗号化システムを概略的に示すブロック図である。

【図12】図11に示される暗号化システムにおける暗号化方法を説明する為のフローチャートである。

【図13】図11に示される暗号化システムにおける他の暗号化方法を説明する為のフローチャートである。

【図14】図14は、図1に示されたメディアデータボックスを暗号化した際の一例を示す平面図である。

【図15】図1に示されたメディアデータボックスを暗号化した際の他の例を示す平面図である。

10

【図16】図1に示されたメディアデータボックスを暗号化した際の更に他の例を示す平面図である。

【図17】この発明の一実施例に係る暗号復号化システムを概略的に示すブロック図である。

【図18】図17に示される暗号復号化システムにおける暗号復号化方法を説明する為のフローチャートである。

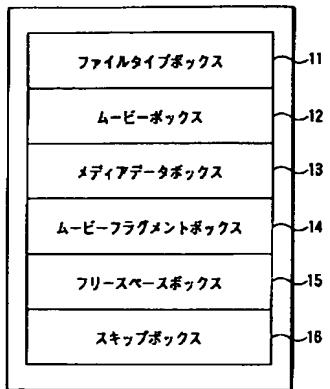
【符号の説明】

1 1 . . .	ファイルタイプボックス
1 2 . . .	ムービーボックス
1 3 . . .	メディアデータボックス
1 4 . . .	ムービーフラグメントボックス
1 5 . . .	フリースペースボックス
1 6 . . .	スキップボックス
2 0 . . .	ボックス
2 1 . . .	サイズ・フィールド
2 2 . . .	タイプ・フィールド
2 3 . . .	ボックスデータ部
1 0 2 . . .	オーディオエンコーダ
1 0 4 . . .	ビデオエンコーダ
1 0 5 . . .	ファイル生成部
1 0 6 . . .	ローカルメモリ
1 0 7 . . .	暗号化部 107
2 0 2 . . .	オーディオデコーダ
2 0 4 . . .	ビデオデコーダ
2 0 5 . . .	ファイル解析部
2 0 6 . . .	ローカルメモリ
2 0 7 . . .	暗号復号化部

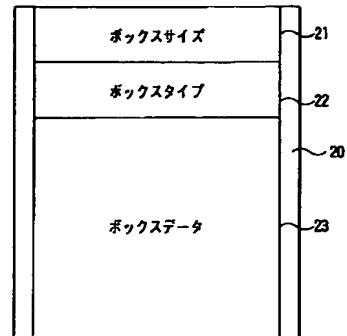
20

30

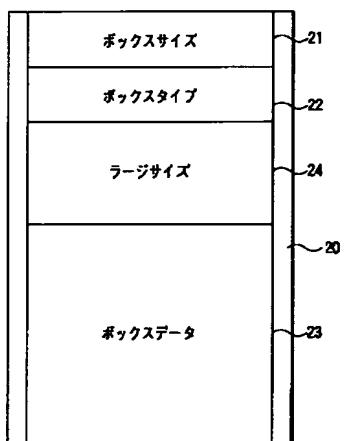
【図 1】



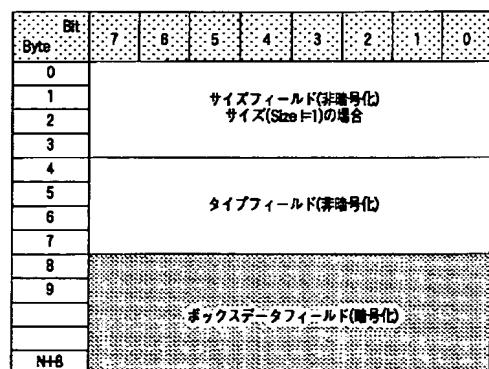
【図 2】



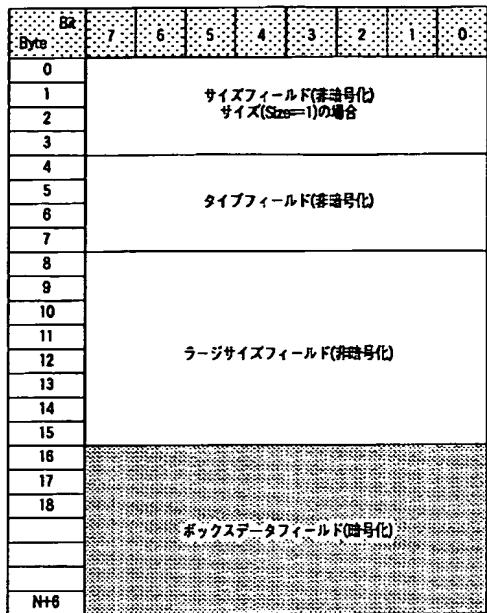
【図 3】



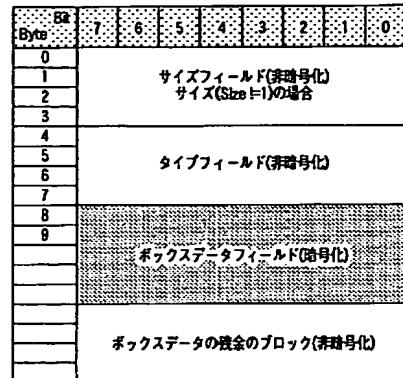
【図 4】



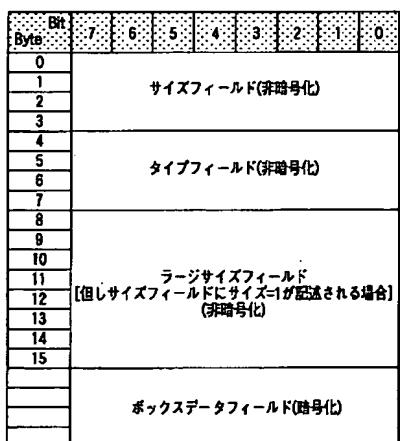
【図 5】



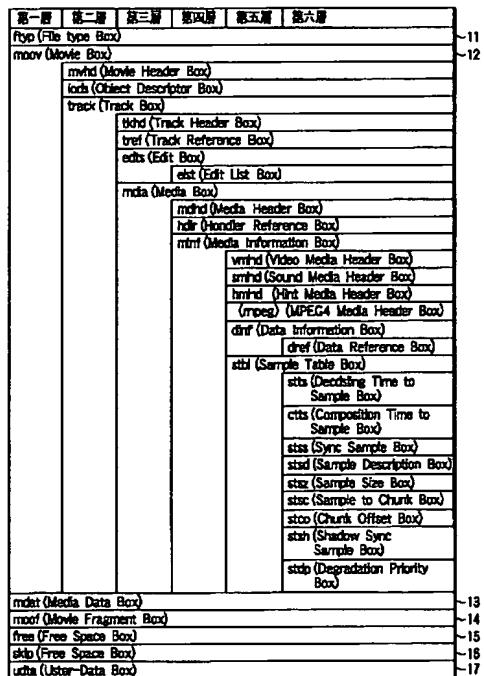
【図 6】



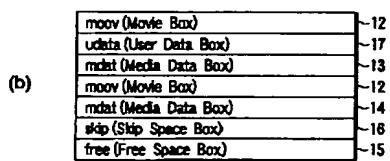
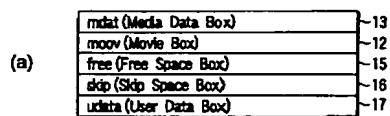
【図 7】



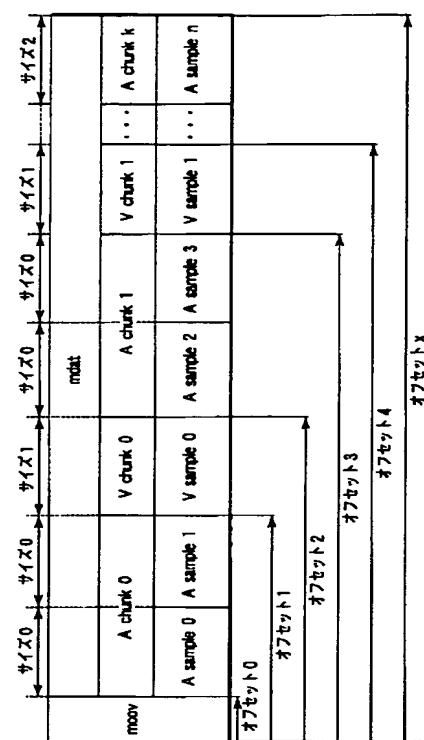
【図 8】



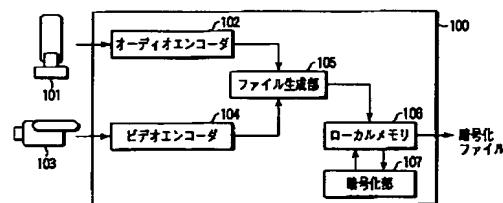
【図 9】



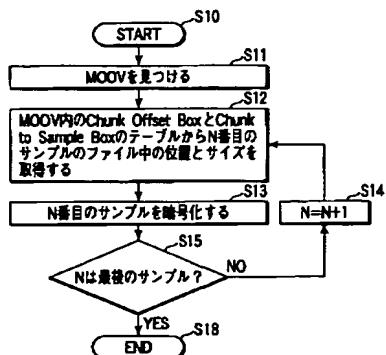
【図 10】



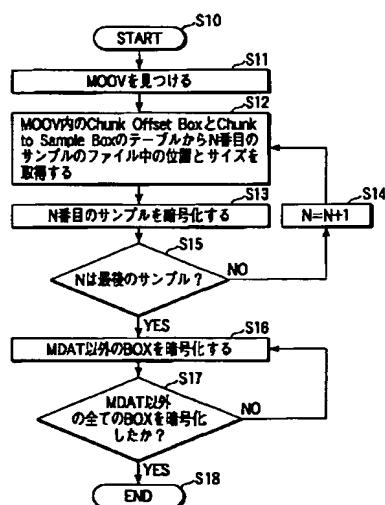
【図 11】



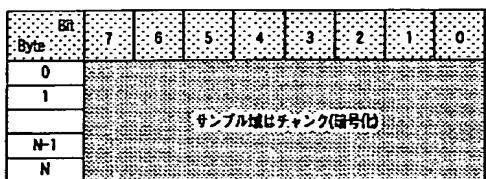
【図 12】



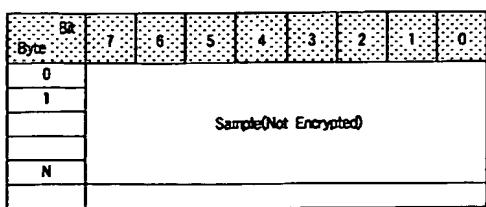
【図 13】



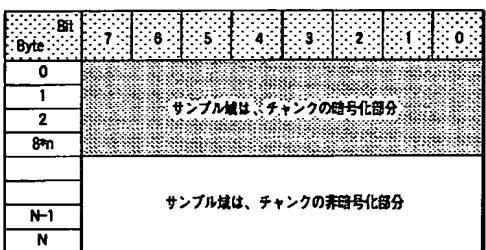
【図 1 4】



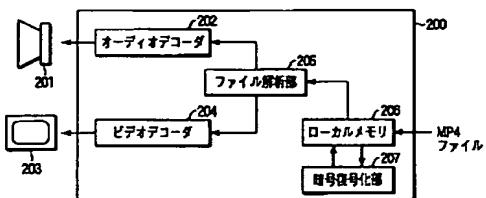
【図 1 6】



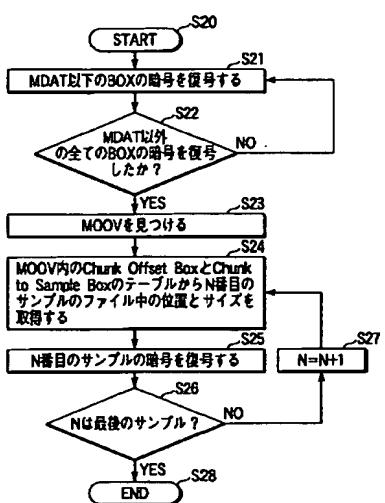
【図 1 5】



【図 1 7】



【図 1 8】



---

フロントページの続き

(72)発明者 佐藤 順

東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内

(72)発明者 寺内 亨

東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内

F ターム(参考) 5B017 AA03 BA07 CA16

SC053 FA13 GB37 HA21

5J104 AA12 AA33 CA02 DA04 NA02 NA27 PA14

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成17年2月17日(2005.2.17)

【公開番号】特開2004-7533(P2004-7533A)

【公開日】平成16年1月8日(2004.1.8)

【年通号数】公開・登録公報2004-001

【出願番号】特願2003-92358(P2003-92358)

【国際特許分類第7版】

H 04 N 5/92

G 06 F 12/14

G 09 C 1/00

【F I】

H 04 N 5/92 H

G 06 F 12/14 3 2 0 B

G 09 C 1/00 6 6 0 D

【手続補正書】

【提出日】平成16年3月9日(2004.3.9)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

第1のポックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のポックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及びマルチメディア・データを格納するデータ・フィールドを含む第1のポックスと、第2のポックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のポックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のポックスのデータ・フィールドに格納されたマルチメディア・データに関する情報データを格納するデータ・フィールドを含む第2のポックスとから構成され、少なくとも前記第1のポックスのデータ・フィールドに格納されたマルチメディア・データが暗号化されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造。

【請求項2】

前記第1または第2のポックスは、サイズ・フィールドに所定の値が設定されているとき、当該サイズ・フィールドが表現できるポックスのサイズよりも大きなサイズを表現するロングサイズ・フィールドを含むことを特徴とする請求項1記載のマルチメディア・ファイル・フォーマットのデータ構造。

【請求項3】

前記第1のポックスにおいて、前記マルチメディア・データの音声または画像の符号化データは所定のサンプル単位でデータ・フィールドに格納され、当該符号化データは、サンプル単位で暗号化されていることを特徴とする請求項1又は2に記載のマルチメディア・ファイル・フォーマットのデータ構造。

【請求項4】

前記サンプル単位の符号化データに対する暗号化は、所定のバイト単位で処理され、符号化データが前記所定のバイト単位に満たない部分を含むとき、当該バイト単位に満たない部分は暗号化されていないことを特徴とする請求項3記載のマルチメディア・ファイル・

フォーマットのデータ構造。

【請求項 5】

前記第1のボックスにおいて、前記マルチメディア・データの音声または画像の符号化データは所定のサンプル単位に分割され、サンプル単位に分けられた符号化データを複数含むチャンク単位でデータ・フィールドに格納され、前記符号化データはチャンク単位で暗号化されていることを特徴とする請求項1又は2に記載のマルチメディア・ファイル・フォーマットのデータ構造。

【請求項 6】

前記チャンク単位の符号化データに対する暗号化は、所定のバイト単位で処理され、符号化データが前記所定のバイト単位に満たない部分を含むとき、当該バイト単位に満たない部分は暗号化されていないことを特徴とする請求項5記載のマルチメディア・ファイル・フォーマットのデータ構造。

【請求項 7】

符号化されたマルチメディア・データを、第1のサイズ・フィールド、第1のタイプ・フィールド、及び第1のボックスのデータ・フィールドを含む第1のボックスと、第2のサイズ・フィールド、第2のタイプ・フィールド、及び第2のボックスのデータ・フィールドを含む第2のボックスとを有するファイル・フォーマット化する方法であって、

前記符号化されたマルチメディア・データを暗号化して第1のボックスのデータ・フィールドに格納し、

前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報を第2のボックスのデータ・フィールドに格納し、

前記第1および第2のボックスのサイズを示すサイズ情報それぞれを、前記第1および第2のサイズ・フィールドに格納し、

前記第1および第2のボックスの種別を識別するためのタイプ情報それぞれを、前記第1および第2のタイプ・フィールドに格納することを特徴とするフォーマット方法。

【請求項 8】

前記符号化されたマルチメディア・データの音声データまたは画像データを所定のサンプル単位に分割し、当該サンプル単位で分割された符号化データをサンプル単位で暗号化して前記第1のボックスのデータ・フィールドに格納することを特徴とする請求項7のフォーマット方法。

【請求項 9】

前記サンプル単位の符号化データに対する暗号化は、所定のバイト単位で処理し、符号化データが前記所定のバイト単位に満たない部分を含むとき、当該バイト単位に満たない部分に対しては暗号化処理しない特徴とする請求項8記載のフォーマット方法。

【請求項 10】

前記符号化されたマルチメディア・データの音声データまたは画像データを所定のサンプル単位に分割し、当該サンプル単位に分割された音声データまたは画像データを複数含むチャンク単位でデータ・フィールドに格納し、当該チャンク単位で暗号化することを特徴とする請求項7のフォーマット方法。

【請求項 11】

前記チャンク単位の符号化データに対する暗号化は所定のバイト単位に処理し、符号化データが前記所定のバイト単位に満たない部分を含むとき、当該バイト単位に満たない部分は暗号化処理を行わないことを特徴とする請求項10記載のフォーマット方法。

【請求項 12】

符号化されたマルチメディア・データを、第1のサイズ・フィールド、第1のタイプ・フィールド、及び第1のボックスのデータ・フィールドを含む第1のボックスと、第2のサイズ・フィールド、第2のタイプ・フィールド、及び第2のボックスのデータ・フィールドを含む第2のボックスとを有するファイル・フォーマットにフォーマット化する装置であって、

前記符号化されたマルチメディア・データを暗号化して第1のボックスのデータ・フィールドに格納する暗号化部と、

前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報を第2のボックスのデータ・フィールドに格納する第1の格納部、

前記第1および第2のボックスのサイズを示すサイズ情報をそれぞれを、前記第1および第2のサイズ・フィールドに格納する第2の格納部と、

前記第1および第2のボックスの種別を識別するためのタイプ情報をそれぞれを、前記第1および第2のタイプ・フィールドに格納する第3の格納部とを備えたことを特徴とするフォーマット化装置。

**【請求項13】**

前記暗号化部は、前記マルチメディア・データの音声または動画の符号化データを所定のサンプル単位に分割してから暗号化することを特徴とする請求項12記載のフォーマット化装置。

**【請求項14】**

前記サンプル単位に分割された符号化データに対する暗号化は所定のバイト単位で行い、符号化データが前記所定のバイト単位に満たない部分を含むとき、前記暗号化部は、前記バイト単位に満たない部分に暗号化処理を施さないことを特徴とする請求項13記載のフォーマット化装置。

**【請求項15】**

前記暗号化部は、前記マルチメディア・データの音声または動画の符号化データを所定のサンプル単位に分割するとともに、当該サンプル単位に分割された符号化データを複数含むチャンク単位とし、当該チャンク単位に暗号化することを特徴とする請求項12記載のフォーマット化装置。

**【請求項16】**

前記チャンク単位に分けられた符号化データに対する暗号化は所定のバイト単位で行い、符号化データが前記所定のバイト単位に満たない部分を含むとき、前記暗号化部は、前記バイト単位に満たない部分に暗号化処理を施さないことを特徴とする請求項15記載のフォーマット化装置。

**【請求項17】**

第1のボックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及び暗号化されたマルチメディア・データを所定のサンプル単位に分けチャンクとして格納するデータ・フィールドを含む第1のボックスと、第2のボックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報データを格納するデータ・フィールドを含む第2のボックスとから構成されるマルチメディア・ファイルを復号化する方法であって、

前記第2のデータ・フィールドに格納されている情報データを読み出し、

前記情報データに基づいて前記第1のデータ・フィールドに格納されている前記暗号化されたマルチメディア・データの少なくとも一部を復号化することを特徴とする復号化方法。

**【請求項18】**

第1のボックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及び暗号化されたマルチメディア・データを所定のサンプル単位に分けチャンクとして格納するデータ・フィールドを含む第1のボックスと、第2のボックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報データを格納するデータ・

フィールドを含む第2のポックスとから構成されるマルチメディア・ファイルを復号化する復号化装置であって、

前記第2のデータ・フィールドに格納されている情報データを抽出する抽出部と、前記情報データに基づいて前記第1のデータ・フィールドに格納されている前記暗号化されたマルチメディア・データの少なくとも一部を復号化する復号化部とを具備することを特徴とする復号化装置。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

【課題を解決するための手段】

この発明によれば、

第1のポックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のポックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及びマルチメディア・データを格納するデータ・フィールドを含む第1のポックスと、第2のポックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のポックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のポックスのデータ・フィールドに格納されたマルチメディア・データに関する情報データを格納するデータ・フィールドを含む第2のポックスとから構成され、少なくとも前記第1のポックスのデータ・フィールドに格納されたマルチメディア・データが暗号化されることを特徴とするマルチメディア・ファイル・フォーマットのデータ構造が提供される。

上述したマルチメディア・ファイル・フォーマットでは、ポックスを単位にデータが格納され、しかも、第1のポックスのデータ・フィールドに格納されたマルチメディア・データが暗号化されている。従って、暗号を解くことなく迅速にポックスをアクセスでき、その内のフィールドに効率的にアクセスすることができる。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

この発明によれば、

符号化されたマルチメディア・データを、第1のサイズ・フィールド、第1のタイプ・フィールド、及び第1のポックスのデータ・フィールドを含む第1のポックスと、第2のサイズ・フィールド、第2のタイプ・フィールド、及び第2のポックスのデータ・フィールドを含む第2のポックスとを有するファイル・フォーマットにフォーマット化する方法であって、

前記符号化されたマルチメディア・データを暗号化して第1のポックスのデータ・フィールドに格納し、

前記第1のポックスのデータ・フィールドに格納されたマルチメディア・データに関する情報を第2のポックスのデータ・フィールドに格納し、

前記第1および第2のポックスのサイズを示すサイズ情報をそれぞれ、前記第1および第2のサイズ・フィールドに格納し、

前記第1および第2のポックスの種別を識別するためのタイプ情報をそれぞれ、前記第1および第2のタイプ・フィールドに格納することを特徴とするフォーマット方法が提供される。

上述したフォーマット方法によれば、マルチメディア・データを暗号化して第1のポック

スのデータ・フィールドに格納し、その他の情報が第1及び第2のボックス内における他のフィールドに格納されている。従って、フォーマットが容易であると共に暗号を解くことなく迅速にボックスをアクセスでき、その内のフィールドに効率的にアクセスすることができるフォーマット方法を実現することができる。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

この発明によれば、

符号化されたマルチメディア・データを、第1のサイズ・フィールド、第1のタイプ・フィールド、及び第1のボックスのデータ・フィールドを含む第1のボックスと、第2のサイズ・フィールド、第2のタイプ・フィールド、及び第2のボックスのデータ・フィールドを含む第2のボックスとを有するファイル・フォーマットにフォーマット化する装置であって、

前記符号化されたマルチメディア・データを暗号化して第1のボックスのデータ・フィールドに格納する暗号化部と、

前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報を第2のボックスのデータ・フィールドに格納する第1の格納部、

前記第1および第2のボックスのサイズを示すサイズ情報それぞれを、前記第1および第2のサイズ・フィールドに格納する第2の格納部と、

前記第1および第2のボックスの種別を識別するためのタイプ情報それぞれを、前記第1および第2のタイプ・フィールドに格納する第3の格納部とを備えたことを特徴とするフォーマット化装置が提供される。

上述したフォーマット装置によれば、マルチメディア・データを暗号化して第1のボックスのデータ・フィールドに格納し、その他の情報が第1及び第2のボックス内における他のフィールドに格納されている。従って、フォーマットが容易であると共に暗号を解くことなく迅速にボックスをアクセスでき、その内のフィールドに効率的にアクセスすることができるフォーマット装置を実現することができる。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

この発明によれば、

第1のボックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及び暗号化されたマルチメディア・データを所定のサンプル単位に分けチャネルとして格納するデータ・フィールドを含む第1のボックスと、

第2のボックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報をデータを格納するデータ・フィールドを含む第2のボックスとから構成されるマルチメディア・ファイルを復号化する方法であって、

前記第2のデータ・フィールドに格納されている情報をデータを読み出し、

前記情報をデータに基づいて前記第1のデータ・フィールドに格納されている前記暗号化されたマルチメディア・データの少なくとも一部を復号化することを特徴とする復号化方法が提供される。

上述した復号化方法によれば、第2のボックスがアクセスされてその内の第2のデータ・フィールドから情報データが読み出され、この情報データに基づいて、第1のボックスのデータ・フィールドに格納されたマルチメディア・データが復号化される。従って、ボックス内の暗号化データを迅速にアクセスすることができ、その内の暗号化データを効率的に複合化することができる。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

この発明によれば、

第1のボックスのサイズを示すサイズ情報を格納する第1のサイズ・フィールド、当該第1のボックスの種別を識別するためのタイプ情報を格納する第1のタイプ・フィールド、及び暗号化されたマルチメディア・データを所定のサンプル単位に分けチャネルとして格納するデータ・フィールドを含む第1のボックスと、第2のボックスのサイズを示すサイズ情報を格納する第2のサイズ・フィールド、当該第2のボックスの種別を識別するためのタイプ情報を格納する第2のタイプ・フィールド、及び前記第1のボックスのデータ・フィールドに格納されたマルチメディア・データに関する情報データを格納するデータ・フィールドを含む第2のボックスとから構成されるマルチメディア・ファイルを復号化する復号化装置であって、

前記第2のデータ・フィールドに格納されている情報データを抽出する抽出部と、前記情報データに基づいて前記第1のデータ・フィールドに格納されている前記暗号化されたマルチメディア・データの少なくとも一部を復号化する復号化部とを具備することを特徴とする復号化装置が提供される。

上述した復号化装置によれば、第2のボックスがアクセスされてその内の第2のデータ・フィールドから情報データが読み出され、この情報データに基づいて、第1のボックスのデータ・フィールドに格納されたマルチメディア・データが復号化される。従って、ボックス内の暗号化データを迅速にアクセスすることができ、その内の暗号化データを効率的に複合化することができる。